Orichalcos

TRANSITIONS FROM REAL TO CRYPTO

Beyond Games: Blockchain Platform with Self-Stabilizing Property Governance

V1.0

Sungho Kim, Ph.D.
(CEO and Founder)

昔者莊周夢為蝴蝶。 栩栩然蝴蝶也。 自喻適志與。 不知周也。俄然覺、則蘧蘧然周也。
不知、周之夢為蝴蝶與、蝴蝶之夢為周與。 周與蝴蝶、則必有分矣。 此之謂物化。

Once upon a time, I, Chuang Chou, dreamt I was a butterfly, fluttering hither and thither, to all intents and purposes a butterfly. I was conscious only of my happiness as a butterfly, unaware that I was Chou. Soon I awaked, and there I was, veritably myself again.
Now I do not know whether I was then a man dreaming I was a butterfly, or whether I am now a butterfly, dreaming I am a man. Between a man and a butterfly there is necessarily a distinction. The transition is called the transformation of material things.

- Zhuangzi (莊子)

-

Contents

IMPORTANT NOTICE

This document is a whitepaper (“white paper”) which contains pertinent information about platform development related to present, future project and suggested ORIC Token ("ORIC token" or "token") Issuance ("Token Issuance Event" or "TGE") of the Orichalcos Foundation ("Orichalcos" or "Foundation") for the potential token holders.

No Information on Orichalcos’ technical whitepaper is deemed to constitute a guideline for inducing or suggesting an investment and is not a suggestion or solicitation to buy investment securities in any jurisdiction in any way

This white paper does not aim to distribute, publish, use or distribute to individuals or entities who are residents of any state, country, or other jurisdiction that is against to the law.

The manner in which this white paper is distributed may be restricted by the laws or regulations of certain countries.

Anyone holding this white paper should notify and follow these suggestions themselves. By accessing this white paper, the recipients of this white paper agree to comply with the restrictions provided by this white paper.

The information in this white paper is generally considered reliable, there is no assurance for the accuracy or reliability of the information and does not imply a contractual relationship factor. The only purpose of this white paper is to provide relevant and reasonable information to potential token holders so that they can decide whether to go through a thorough analysis of the Foundation, the project and the platform with the intention of obtaining an ORIC token.

This White Paper is for informational purposes only and is not intended as an explanation of future intent.

This White Paper is only available from www.orichalcos.io and may not be redistributed, reproduced, or transmitted to anyone, or in whole or in part, for any purpose without the prior written consent of Orichalcos

---

This white paper attempted to reflect our plans as much as possible, but it can change as the project progresses. This white paper can also be modified. Please check the website for the latest version.

If you are uncertain about this white paper or have any questions, please seek advice from an attorney, tax accountant, or other specialist. It is a good idea to read the entire white paper and be familiar with all of the information described below. In particular, please be sure to read the final "Danger and Disclaimer".

Orichalcos Foundation

The Orichalcos Foundation was established in Seychelles for the Orichalcos project. All donations received by Foundation through the token generation event (TGE) will be used to support the Orichalcos project and roadmap.

Orichalcos Foundation may work with various contractors to achieve its objective as well as to realize collaboration possibilities in the global community.

Registration No.: 000744

Address: 103 Sham Peng Tong Plaza, Victoria, Mahe, Seychelles

Abstract

Orichalcos is a private blockchain platform that can be used in game and other incentivizable areas.

Recognizing the user's right on asset distribution and in-game history, Orichalcos rewards with the currency called ORIC Stone which circulates within the platform in exchange for the effort and time of the users spent on the creation of new game data. This kind of self-stabilized reward for gameplay induces the game to be enjoyed deeply enough and stimulates participation in new games.

The ecosystem of Orichalcos platform starts with ORIC Stone which is supplied through platform, will contribute to the game vitalization by consumption in item trading and various in-game contents. In addition, in the external exchange it can be made to an ORIC Token which is cryptocurrency. Game data will be archived and given to each user, which enables to preserve their game history and serves as a bridge between past and present.

For example, users can receive ORIC Stone in exchange for sharing their own game data to developers. And it will be utilized by developers to in advertising and operating strategies to provide more precise game services and Orichalcos also provides target marketing tools and user analysis console. In our ecosystem based on game data, the user's history will be created from the game provided by the developer. That history will be processed into game bigdata on the private blockchain network and provided to the developer again. In this process, the value of the game experience is transformed into ORIC Stone and as a result, it creates circulation structure within the platform ecosystem. The Orichalcos ecosystem becomes bigger with the reliability of game data as the number of users in the platform increase. It will lead to more active circulation of ORIC Stone, which will contribute to the value of ORIC Token. Thus, by combining game software with blockchain technology, Orichalcos want to build a circulative structure that allows users, developers, and platforms progress mutually.

In view of technical aspect, Orichalcos utilizes a permissioned blockchain technology. In order to develop the platform a public blockchain Hyperledger was chosen. In addition, we will introduce a consensus algorithm that combines PoET with hierarchical Raft consensus algorithm to develop permission-less public blockchain in future. For the Dual Token and blockchain system, ORIC Token and ORIC Stone, after issuing Ethereum ORIC Token will be pegged to Hyperledger blockchain will be used as a starter. The modified and pegged Hyperledger blockchain will issue ORIC Stone. We will use Oracle to supply data to the blockchain network to take advantage of centralized external data. After separating user data from Distributed Ledger Layer in order to operate network efficiently, user data will be stored in distributed shared storage like IPFS (Inter-Planetary File System) or Storj.

In order to maintain low volatility against external fiat currency, we will operate the ACB (Algorithmic Central Bank) for ORIC Stone within the platform. Therefore, after the ORIC Token Generation Event is finished to maintain the Token value in the private blockchain, the remaining tokens will be kept in the Central Treasury. The token economy is designed so that the value of the token increases as the platform value grows.

The entire system will be configured as a cloud system, and approval for blockchain transactions will be made in an authorized node distributed worldwide. In order to develop into separate public blockchain in the future, incentives for participating nodes should be designed and reflected.

1 Introduction

1.1 Overview of Blockchain

In Jan. 2017 Harvard Business Review, Marco Iansiti and Karim R. Lakhani begin their article on the blockchain (Marco & Karim, 2017)

> *Contracts, transactions, and the records of them are among the defining structures in our economic, legal, and political systems. They protect assets and set organizational boundaries. They establish and verify identities and chronicle events. They govern interactions among nations, organizations, communities, and individuals. They guide managerial and social action. And yet these critical tools and the bureaucracies formed to manage them have not kept up with the economy's digital transformation. They're like a rush-hour gridlock trapping a Formula 1 race car. In a digital world, the way we regulate and maintain administrative control has to change.*
>
> *Blockchain promises to solve this problem. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.*

In addition, they have mentioned that ***Blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems*** (Ephraim, 2018). People sometimes claim that blockchain will add greater visibility and efficiency across the entire supply chain to deliver higher value to your customers and trading relationships (Anon., 2018); will track ownership of real estate (Steve, 2017); and could revolutionize the Internet of Things (Jason, 2017).

There is no explicit description of the blockchains in the cited applications. But the blockchains of cryptocurrencies are well understood. As Satoshi Nakamoto writes, they are needed to enable "electronic transactions without relying on trust." A complete, immutable public record of transactions is not a design goal in cryptocurrencies (Nakamoto, 2008). Nakamoto wrote that "To accomplish this without a trusted party, transactions must be publicly announced." (Dai, 1998)

So how do we define a blockchain? Ephraim Feig, IEEE Life Fellow, defines the blockchain and the blockchain network as follows (Ephraim, 2018):

***Definition**: A blockchain is a sequence of blocks of data in which each block, other than the first, is cryptographically linked to its predecessor.*

***Definition**: A blockchain network is a peer-to-peer network in which peers collaborate to achieve a common goal by using a blockchain.*

The idea of chaining blocks of data together with cryptographic hashes has been around since the late 1970's. (I will restate the cryptographic hashes simply later at the tokenization section.) The cryptographic protocols were evolving by 1982, when Ralph Merkle's patent was granted (Ralph, 1980). The data structure named after him, the Merkle Tree, found utility in peer-to-peer systems in which peers all needed to share identical data.

1.2 Evolution from Blockchain to Bitcoin

For the history of cryptocurrency before the Bitcoin, J. Bonneau and et. al summarized in their review paper (Bonneau, et al., 2015).

In short, cryptographic currencies date back to Chaum's proposal for "untraceable payments" in 1982 (Chaum, 1982), a system involving bank-issued cash in the form of blindly signed coins. Blind signatures prevent the bank from linking users to coins, providing unlinkability akin to cash. Throughout the 1990s, many variations and extensions of this scheme such as removing the need for the bank to be online at purchase time, allowing coins to be divided into smaller units (Okamoto & Ohta, 1992) were proposed. DigiCash and Peppercoin attempted to bring electronic cash protocols into practice but ultimately failed in the market.

Proof-Of-Work (POW) puzzles was proposed for combating email spam in the early 1990s (Dwork & Naor, 1992) and after many other applications followed, including proposals for a fair lottery (Goldschlag & Stubblebine, 1998), minting coins for micropayments and so on. POW was also used to detect sybil nodes in distributed peer-to-peer consensus protocols (Aspnes, et al., 2005).

The public ledger, essential element of Bitcoin makes double-spending detectable. In the late 1990s, auditable electronic cash (Sander, et al., 2001) proposed, the bank maintains a public database to detect double-spending and ensure the validity of coins. B-money (Dai, 1998) that proposed in 1998, appears to be the first system where all transactions are publicly and anonymously broadcast.

Smart contracts (Szabo, 1997), proposed in the early 1990s, enable parties to formally specify a cryptographically enforceable agreement, portending Bitcoin's scripting capabilities.

In 2008, Bitcoin was announced, and a white paper penned under the pseudonym Satoshi Nakamoto was posted to the Cypherpunks mailing list (Nakamoto, 2008), followed quickly by the source code of the original reference client. Bitcoin's genesis block was mined on or around January 3, 2009. 2 The first use of Bitcoin as a currency is thought to be a transaction in May 2010, where one user ordered pizza delivery for another in exchange for 10,000 bitcoins. Since then, an increasing number of merchants and services have adopted Bitcoin.

The technical aspects of the Bitcoin are briefly summarized below.

Blocks of Bitcoin generated about every 10 minutes are connected as long as the chain. Each block consists of timestamp, nounce, hash value of previous block and transaction contents. The timestamp means when the block was generated, and it is also used to prevent the hacking. The nounce which is generated with SHA256 algorithm is 4 bytes and is used to adjust the hash values.

Bitcoin is one of the best samples but has some disadvantages. Those are Turing incompleteness, value blindness and verification time. Turing incompleteness is simply the inability to use the ***while*** and ***for*** statements. The bitcoin also has a script, but it is equipped with an OPCODE that can execute only a simple command. There is

also an advantage of preventing DDOS[1] attack because it does not include these repetition commands.

If you look at bitcoin as a currency, you should know its value. For example, when you convert a dollar into bitcoins, and then try to convert the bitcoins back into dollars after 30 days, you need to know the value of the dollar that corresponds to the bitcoin, but there is no easy way to know, i.e. there is value blindness.

As described above, in the case of bitcoin, it takes about 10 minutes to generate one block. When a block is created, it says that it has been verified, and as the number of verifications increases, the credit of the transaction also increases. It means that ten verifications can be more reliable than three verifications. People can wait about an hour for a big deal, but it's not common to wait an hour for a cup of coffee. The long time to finalize the transaction is not only a bitcoin but also a disadvantage of all cryptocurrency (Garay, et al., 2017).

1.3 The Second Generation of Cryptocurrency: Ethereum

One of the most successful blockchain technology is Ethereum. Ethereum was proposed by Vitalik Buterin in 2013 (Buterin, 2013). In mid-2015, after its first public release, it became the second largest cryptocurrency in a short period of time, receiving much acclaim. In the case of Ethereum, one block is generated at approximately 12.4 seconds. Unlike Bitcoin or other cryptocurrencies, Smart Contract has had a major impact on Ethereum's success. By incorporating the smart contract, first proposed by cryptologist Nick Szabo in 1994 (Szabo, 1997), into a blockchain, Ethereum provided an environment in which to execute programs using Turing complete computing capabilities and their functions in addition to the basic transaction record.

However, Ethereum has been a tremendous success in less than three years since it was introduced, but it has been attacked by DAO Attack, OPCODE Computational DDOS Attack, and so on. Compared to other blockchains, it still has a lot of attacks because of its complex structure.

In the case of Ethereum, it is significant not only to record transaction from A to B, but also to add a computing function while compensating for the disadvantage of Bitcoin. Ethereum developers define ***Ethereum as a built-in Turing-complete programming language*** (Buterin, 2013). That is, there is a property that a program can be implemented or executed in a blockchain. Thus, Ethereum has a more complex structure than bitcoin.

Ethereum also has the same concept as the wallet of Bitcoin. However, unlike Bitcoin, there are two kinds of accounts, Externally Owned Account and Contract Account. EOA[2] is the same concept as the coin of a Bitcoin. Address exists and Ether which is Ethereum's currency unit is included. A public and private key is created based on ECDSA[3]. CA[4] is one of the accounts of the asset. Generally, the EOA is used

[1] DDOS: Distributed Denial of Service

[2] EOA: Externally Owned Account

[3] ECDSA: Elliptic Curve Digital Signature Algorithm

[4] CA: Contract Account

as the user 's wallet, but the CA exists inside the blockchain and has several characteristics. First, it can contain codes, and it can execute codes outside or inside the blockchain. Second, you can store the data. And like any other EOA, you can own an Ether.

For the Ethereum blockchain, there is an EVM, Ethereum Virtual Machine. Ethereum actually has programming languages such as Solidity and Serpent, and the program can be implemented using those language. After compiling the program, it is converted into bytecode, and there is an operation code corresponding to the bytecode. Another interesting thing is Turing-complete computing capability. As mentioned earlier, by running code like while (1) {}, you can simply do DDOS attacks. Due to the nature of the blockchain, the participating miner will verify and execute the code, so that the blockchain itself can be paralyzed when executed on all machines participating in the above code.

To solve this problem, there is a concept of gas. Because there is a gas price per operation code, you have to set the amount of gas when you run the code first. For example, when you run a program with 10000 gas, you will not be able to run the code to the end if you run out of gas. Hence, if you want to execute code like while (1) {}, you should consume as much astronomical or infinite amount of Ether.

Because the blockchain is nearly immutable and permanent, if it is possible to run a program in a blockchain, such as Ethereum, rather than a general distributed ledger, we can get many advantages. First, you can trust your code on Ethereum. The code that works on a regular server does not know exactly what is going on in the real server. If all the code and the steps to be executed are made visible to the blockchain participants, users will be able to trust the service. Second, the stored code and data remain "almost" permanently. For this reason, it can be used as permanent storage of data that should not be modulated. A program running in the Ethereum blockchain is called a Decentralized Application or DApp. The Ethereum ecosystem is currently the best place to build a decentralized application; it has wonderful documentation and user-friendly interfaces, fast development time, security for small applications, and ability for applications developed atop the Ethereum blockchain to easily interact with one another.

1.4 Other Blockchain and Cryptocurrency

Until now, much attention has been paid to the dramatic characteristics of Ethereum, but many blockchain technology are being developed in addition to Ethereum. I will briefly discuss the representative Hyperledger project, R3CEV's Corda, and ZCash.

Hyperledger started in December 2015 at the Linux Foundation. The majority of existing blockchain are associated with cryptocurrency. This blockchain has various uses as a public blockchain, but there are obvious limitations. For example, a blockchain that is available only to specific people, and a public blockchain that anyone can use can be said to be quite different. So, to make up for the limit of many existing public blockchain, Hyperledger was made. There are several projects in Hyperledger. In order to solve real-time-sensitive service problems, projects such as the development of a stable system capable of processing real-time high-volume transactions and the construction of a blockchain of a consortium type are underway.

IBM, Intel, and VMWare, as well as financial / banking companies such as JP Morgan and BNY Mellon are also participating.

Hyperledger Blockchain for applications other than currencies are developed even further in conforming to standard trust models. Permissioned-blockchains have been suggested for enterprise applications, in which "participants need to obtain an invitation or permission to join. The access control mechanism could vary: existing participants could decide future entrants; a regulatory authority could issue licenses for participation; or a consortium could make the decisions instead." Moving even further from trust averse systems, we have private networks that are not only permissioned but also restrict who can see the blockchain.

R3CEV is currently the largest block-chain consortium for the financial sector. Deutsche Bank, Nomura, Barclays, Credit Swiss and more than 50 companies are participating. It was created to simplify the complex transactions and functions required in the financial sector by using a blockchain. To accomplish this purpose, a project named Corda was released and the source was released openly.

ZCash is a cryptocurrency that was released in October 2016. It has features that are different from the existing Bitcoin or Ethereum. An existing public blockchain claims to guarantee anonymity, but it does not know who created the account, and because the transaction history in the blockchain can be fully identified, the recipient, sender, and amount can be known. Hence perfect anonymity is not guaranteed. ZCash, however, has the advantage to hide all recipients, senders, and amounts by using the Zero-Knowledge Proof. (Seyoung, et al., 2017)

1.5 Smart Contract: A Way From Real To Crypto

We already know the definition of **contract** which provides parties with a set of rights and obligations, which are used among other things to encourage long-term relationships. This is very useful in environments where relationships thrive upon trust (Morabito, 2017). Nick Szabo extended this definition of contract to the blockchain and defined **smart contract** in his article "Smart Contracts: Building Blocks for Digital Markets" as follows (Szabo, 1997):

> ***"A set of promises, specified in digital form, including protocols within which the parties perform on these promises."***

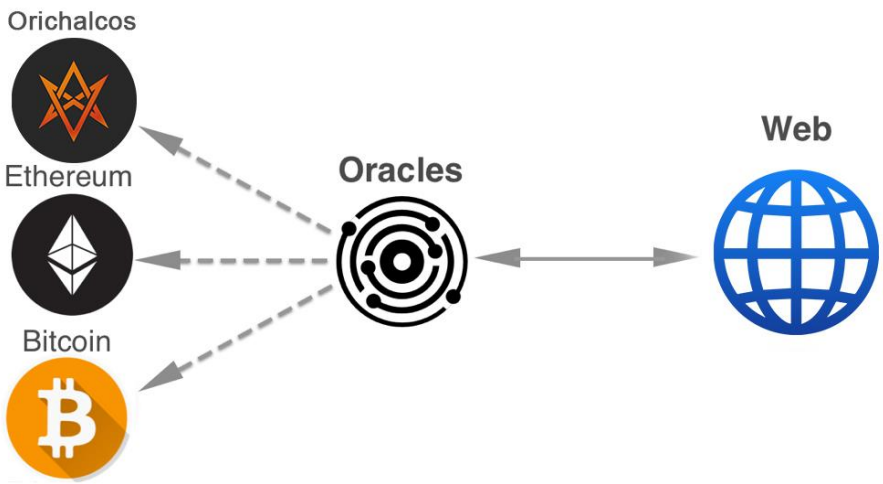
In short, it refers to an "automated trade agreement" that automatically runs without human intervention if the conditions specified in the contract are programmed. Morabito divided smart contracts into two types: deterministic and nondeterministic (Morabito, 2017). A **deterministic smart contract** is a type of contract that does not have any data from the outside of blockchain, while **non-deterministic smart contract** is a form that requires external data in its execution. Non-deterministic Smart contracts are vulnerable to security breaches compared to deterministic smart contracts which is no need for external data, because they need to retrieve data from external systems rather than from blockchain networks. Non-deterministic smart contracts, however, can be integrated with external systems to create various types of smart contracts and automation implemented, a very important element of smart contracts. (Ahn, 2018)

For example, in Ethereum Smart Contract, it runs in a way that subtracts a certain amount from the gas paid in advance, so you cannot deliberately delay the execution or repeat the calculation indefinitely. Smart contracts written in languages supported by Ethereum run on the Ethereum Virtual Machine (EVM). EVMs that run smart contracts in a non-secure environment where anyone can create and register smart contracts in a public permissive blockchain runs quarantined in a redundant network environment (Buterin, 2013).

Smart contracts are one of the most important key elements in the blockchain technology and cryptocurrency. Szabo explained the idea that smart property might be created by implanting smart contracts in physical objects. Tokenization can be realized through smart contracts. By using the blockchain Smart Contract, you can capitalize all tangible and intangible asset-value into the Token.

1.6 Oracle: Gateway From Real to Crypto

An Oracle is defined as *a person or thing regarded as an infallible authority or guide on something.* In the context of decentralized networks, Oracle source and validate data from the outside world. Smart contracts then utilize Oracle-validated data to function. In general, smart contracts require specific data input from outside sources of decentralized network. **Ensuring the validity of this data is paramount in order for smart contracts to function.** Thus, when it comes to the issue of utilizing off-chain data, **an Oracle acts as an intermediary, a validation and 'formatting' tool, between the data source and data user.**



Indeed, Vitalik Buterin confirmed his view of the importance of Oracles (Buterin, 2014), writing:

"…At other times, however, oracles do make sense. The most common case that will appear in reality is the case of external data… Another important case is smart contracts that actually are very hard to evaluate."

An Oracle is, simply put, a “smart contract” that is able to interact with the outside world, in the world of Ethereum that is known as off-chain.

1.7 Tokenization and Programmable Economy

Tokenization, when applied to data security, is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value. The token is a reference (i.e. identifier) that maps back to the sensitive data through a tokenization system. The mapping from original data to a token uses methods which render tokens infeasible to reverse in the absence of the tokenization system, for example using tokens created from random numbers (Wikipedia, 2018).

However, nowadays, tokenization is used in field of blockchain technology. As usual, **tokenization is the process of converting certain types assets whether it is tangible or intangible into blockchain tokens**. There are all kinds of assets, such as stocks, real estate, rice, automobiles and gold, and so on. People buy and sell them for their own purposes. As technology has developed, different types of assets have begun to emerge, such as copyrights, insurance policies, and derivatives, and have a tradeable value when certain conditions are met. These assets can be replaced with blockchain-based tokens and their ownership can be registered. In addition, if the necessary conditions can be specified through a smart contract, it can be possible to convert into new assets. **Assetization, i.e. Asset tokenization is the process of assigning ownership to intangibles such as game items, credit card points, or even one’s own influence on social medial platforms, such as SNS.**

Widely accepted these phenomena is heralded as **programmable economy**. Gartner created the term **programmable economy** in 2014 to refer to emerging phenomenon. The programmable economy is a natively "smart" economic system that supports and/or manages the production and consumption of goods and services, enabling diverse scenarios of exchange of value — both monetary and non-monetary (Hegadekatti & G., 2017). **The programmable economy, enabled by metacoin platforms and smart technologies**, will support new forms of value exchange, new kinds of markets including dynamically defined on-demand markets (Gartner, 2015).

In the era of programmable economy, where cataclysmic technologies and economies are mixed, the era of new dreams in which realities and virtual assets are transited to each other has come through the blockchain technology.

1.8 Token Economy

The term “Token Economy” is defined in Wikipedia, you will see as follows.

A token economy is a system of contingency management based on the systematic reinforcement of target behavior. The reinforcers are symbols or "tokens" that can be exchanged for other reinforcers. A token economy is based on the principles of operant conditioning and behavioral economics.

According to Wikipedia, there are three essential elements for Token Economy to be established. **Tokens, Back-up Reinforcers, and Specified Target Behaviors. Tokens will be a rewards or penalty in the punishment system, and a cryptocurrency in the crypto**

ecosystem. Back-up Reinforcers are enhancer that is interchangeable with token in the definition. In the punishment system it will be rewards to people who collect the most or punishment, such as cleaning up the toilet for people who have a lot of listings or penalties. In the cryptocurrency ecosystem, it means goods, rewards or cash used in real life. Finally, **Specified Target Behaviors** is important. This is a story about what Token Economy will do for participants. The punishment point system means that you listen to your teacher, keep you quiet in class, and not fight your friends.

The point to note here is that the Token Economy is used to change people's behavioral processes. It is especially effective when there is no definite behavior like students. When Token Economy is organized, you can change the behavior of participants. And you can change behavior to let participants generate value. And the value of Token Economy can be considered to be worth it. On the other hand, this is where many of the most cryptographic ecosystems are missing, and we feel that there is a distance between the cryptographic ecosystem and the punishment system. (joce00, 2018)

On the other hand, Pablo Moreno de la Cova defined Token Economy as follows (Moreno, 2017).

> *The design of a token and the set of rules of the economic ecosystem where it will be used. The key idea is that through a design based on game theory and incentives, the use of the token becomes desirable by all stakeholders of the ecosystem: clients, suppliers and the sponsors of the token.*

Token Economy is often called Tokenomics or Tokenized Economy. As Pablo mentioned Token Economy design the set of rules between token and real-world economic system. As mentioned in the definition of Wikipedia, the key idea is based on game theory and incentive systems, and all token ecosystem participants, including customers, suppliers, and token supporters, are willing to use it. In other words, it refers to an economic structure in which appropriate rewards are paid according to participation in all participants in the token ecosystem (mechuriya, 2018).

1.9 Volatility and Instability of Cryptocurrency

To incorporate all the features of a traditional currency i.e. scarcity, fungibility, divisibility, durability, and transferability into a digital currency, and to utilize it as a medium of exchange, as a unit of account and as a store of value, such digital currency should be more stable than the current state of Bitcoin or gold.

The current value of cryptocurrencies often experiences regular fluctuations rising or falling by about 25% in a single day, and occasionally rising to over 300% in a month. Price volatility of cryptocurrencies is unprecedentedly too high making it unsuitable for everyday usage. If the price of a cryptocurrency is not stable, it will be difficult to utilize it in the credit and debt market. This is because it will attract a large premium as a buffer against price risk in the event that any future contract payment is based on cryptocurrency. Owing to these negative impacts that such price instability has on cryptocurrencies, its utilization is limited.

2 Why Are We Making Orichalcos?

2.1 Issues on game ecosystem

2.1.1 Centrality and Ownership on Gaming

In the past decade, game development has evolved to be designed with online environment, and play data is designed to be stored in a remote server rather than a local storage device. In addition, a series of game assets are also managed by the internal server of the developer or publisher's contracted data center. The rights of the data and resources constituting the game system belongs to the developer, and the ownership of various values generated by the user investing time and effort is also not given to the user.

The developer specifies the right to amend / delete game data and the disclaimer for problems that users have not paid for as required by the operating policy. Furthermore, it has the right to suspend the game service itself and right to get access to any information. In other words, the user's asset may disappear, and services may be put to a stop and/or access to user data is blocked when necessary.

2.1.2 Security and Reservation of History Data

In addition, as a result of the lack of item trading market, gamers resort to utilizing the services of an external company which allows an irrelevant 3rd party to take all the advantage. This trading behavior, which occurs under the negligence of the developer or operator is generally a violation of the item exchange rule, and the user's account may be suspended, and the goods related to the exchange may be deleted.

By itself, gameplay is already an act. The experience that the users have made in game is preserved in the game itself in the form of digital goods and statistics, so the traces should still exist and be memorable over time. However, we know that this data is being controlled and stored by someone else, in most cases by the developers, and could be destroyed or deleted at any time.

2.1.3 High Platform Costs and Opportunity for Success

Many gaming platforms provide promised services such as software package storage and download solutions, advertising promotion services, user account information management and community provisioning necessary for developers to service games, and regularly collect massive fees of up to 30% of total game revenue.

While revenue of these platform-driven businesses increases dramatically by adopting new games, the actual contribution of these platforms to improve the quality of the game is negligible. This is because only the standardized services are provided within the infrastructure built on the platform.

2.1.4 Development Tools and API for blockchain-based games

APIs or development tools for game developers are required with dependents on the access path such as mobile and web. There are various kinds of development tools used for 2D / 3D, advertisement / user tracking, authentication, and data storage. In addition to the game development tools, if you want to use blockchain technology in games, it requires plug-in development tools that utilize it. However, development tools are still insufficient in their specifications in order to develop blockchain based games.

In the end, a game company that wants to lead the market need to share profits with platform companies while at the same time allocating sufficient resources for game development.

2.2 Issues on blockchain and cryptocurrency for gaming platform

2.2.1 Technical limitations of crypto-game

One thing you can see in blockchain games is that public blockchain technology is not enough to handle large amounts of user data efficiently. There were not enough technical attempts, such as introducing a master node or altering the consensus algorithm for fast in-game data processing and transaction authorization, and even crypto games have not been adequately tested for a large number of users.

Crypto-Kitty's purchasing, sales and exchange processes accounted for higher than expected costs of speeding up transactions. Of course, it can be relatively small compared to current platform cost and advertising cost. However, because the user sets the transaction fee and the higher the commission fee, the sooner the transaction is approved, Ethereum commission policy is not suitable for frequent trading areas with micro-transaction, such as games,

Various payment methods exist in the game such as card payment, payment gateway (PG), cash transfer, and telephone bill payment. In addition to using the cryptocurrency in the game, the existing legal currency payment method also must be supported. Users who want to play the game should be able to access and play the same way as existing game.

As mentioned earlier, various kinds of development tools are needed. In addition to game development tools, there is a need for plug-in development tools that can take advantage of the use of blockchain technology in games. However, development tools with detailed specifications for developing blockchain games are still lacking.

2.2.2 Token economy based on high volatile currency

In many areas where transactions occur as well as games, the ability to function as money or currency is essential. Money is any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a particular country or socio-economic context. The main functions of money are distinguished as: a medium of exchange, a unit of account, a store of value and sometimes, a standard of deferred payment. Any item or verifiable record that fulfills these functions can be considered as money. (Wikipeida, 2018)

When purchasing a game item, you will be charged using cash, card vouchers, gift cards or various type of points. Also, the rewards you receive during the game have various forms such as rising levels, new items, and prizes. If the value of the settlement and the rewards are changed according to time or place, the game users think that the policy of game by the developer or the publisher is not fair. They cannot calculate the average value of their efforts and do not play the game.

The value of money and rewards that are encountered through the game should not change as much as possible, even if they are defined in the terms and conditions. The standard of value that should not be changed in this way should be the same as the value of the commonly used currency. The compensation for purchasing an item by paying $ 1 shall be convertible into money.

Consider the case of paying with a gift cards or voucher instead of a dollar. If the price of this gift card or voucher cannot be predicted because the price changes on a daily basis, how can the game user purchase the product with this voucher and pay for the monthly subscription fee?

If you want to implement an economic system of a game platform or game without cryptocurrency, there will be no problem, but if you want to use cryptocurrency, stable monetary value is essential for economic system implementation.

In general, the volatility of cryptocurrency is more than several times higher than the value of traditional fiat currency. It is impossible to design the economic system of the game using these cryptocurrencies, and even if designed, it will not be accessed by game users. The game will become like a cryptocurrency exchange. Only cryptocurrency transactions occur, and users will not be immersed in the game on the platform. For this reason, companies that introduce blockchain technology and cryptocurrency into game platforms will use blockchain and cryptocurrency as compensation for asset exchange and user data leaks or leverage.

2.2.3 Trilemma in blockchain: Decentralization, Scalability and Security

In many fields of data processing as well as block chains, we are always trying to be more available(availability), more scalable(scalability), and more safe(safety). Despite these efforts, however, there may not be cases in which all situations are satisfied.

In designing a system, availability is an indicator of how long the system can operate continuously. However, in order to update system hardware or software on a regular basis, the system must be shut down. That is, the availability becomes low. If you stop checking software or hardware to increase availability, safety will be compromised. Even if availability becomes low, it is necessary to regularly check the hardware and software to enhance the security of the system.

Security is an act to prevent malicious access to the data itself or through defects in the data or at various stages of the processing of the work, and therefore, security checks should be performed at various stages of processing by the system. If you want to increase security level, you must reduce the number of points that can cause malicious access, which limits the scalability of the system. Distributing the centralized system processing functions to multiple locations increases availability with multiplexing, which inevitably reduces security. Decentralization reduces safety and improves scalability and availability.

In this Trilemma situation, all the conditions of the system cannot be satisfied, so the part to focus more have to be decided. Of course, if one of them completely be ignored, the whole system cannot be used. Hence it has to be designed to include at least the portion you want to ignore.

Processing speed is a very important issue in commerce. Minimizing the number of transactions to be processed per second (number of TPS) or the processing time per transaction (second per transaction) is a different problem. These are units of performance of the consensus algorithm that have to be measured separately. Although the performance of consensus algorithms is concentrated on transactions per second recently, the time to completion of each transaction is also an important factor.

2.2.4 Cost of Transaction and Complexity of Transaction Finality

The blockchain adopts cryptography to secure security and stability. In order to establish a contract and a transaction without having middleman, the aim is to reduce the cost incurred by having middleman. However, as the middleman disappeared, the transactions involved only by the transaction parties may be extremely bad because of malicious participants. In order to prevent this, a consensus algorithm was introduced that is agreed upon by the entire participant. P2P communication was further introduced for data processing that must be sent in order to reach consensus or approve contracts or transactions.

> ***Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model.***
>
> ***Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.***
>
> ***A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.***

As mentioned in Bitcoin whitepaper, Direct transactions between sender and receiver, seller and buyer can save unnecessary commissions by eliminating intermediaries, but additional confirmation costs (mining or authorization costs) arise.

In recent years, another type of consensus algorithm has been proposed. However, as many consensus algorithms (DPoS, etc.) including an intermediary broker have appeared, the advantage of the original Bitcoin disappeared, and the system complexity became high. In addition, there is a need to implement a system of consensus algorithms to be performed by participating nodes while minimizing human intervention.

2.2.5 Payment Speed and Micro-transaction

The transactions on the blockchain differ in many ways from the transactions in the game. In particular, the difference in number of transactions can be mentioned. Consider the case of VISA or MasterCard. People shop at a store for a day, eat food and make payments. In the case of home appliances shops, many people visit to buy the washing machines and/or refrigerators in a day, but few customers actually go and check out. But on the other hand, if you think about a lunchtime restaurant, the visitor will be the number of customers who will be paid soon. If the card companies go through the procedure and payment procedure every time they notify the store about all the transactions happening in the store, the card company system will have

to have higher processing speed and capacity. in general, the card company informs and processes the payment once a month or for a given period.

It may be unreasonable for each node to agree on every micro-transaction that occurs on a block chain. In the case of EOS, 21 BP processes all transactions. On the other hand, Ethereum has more than 10,000 nodes handling transactions. As with the extreme two models**, it can be efficient to process microtransactions collectively for the appropriate trading unit or group, just as the current financial system does the remittance through an intermediary bank.** As you know, Facebook handle 157k transactions per second (TPS), Ethereum about 12 TPS, BTC about 7 TPS. However, in order to improve the settlement processing speed, studies on Atomic swap or Sharding are underway while managing these frequent transactions in an integrated manner.

Still, in the case of blockchain games the public blockchain seems to be insufficient to efficiently process large amounts of user data. It has not been verified whether the public blockchain has sufficient processing speed when implemented using other consensus algorithm for in-game data processing and transaction approval, and it has not been tested by massive users, too.

2.3 Needs for Token Beyond Games

As mentioned before, the programmable economy is a term created by research firm Gartner Inc. in 2014 to describe the revolutionary changes happening in the global economy due to technology innovations. (Rouse, 2018) In addition, the term **Tokenization** is used in field of blockchain technology. As usual, **tokenization is the process of converting certain types of assets into blockchain tokens**. There are all kinds of assets, such as stocks, real estate, rice, automobiles and gold, and so on. These assets can be replaced with **blockchain-based tokens** and their ownership can be registered, and if the necessary conditions can be specified, through a smart contract it can be possible to convert into new assets.

In general, various forms of money are used in games. Let's say the game money to be received while playing the game is Gold. Gold is the economic unit if the basic monetary unit of the game. As the game progresses, you can purchase or enhance items to play the game with this Gold. Paid items can be bought by collecting a lot of Gold, but sometimes cannot be bought. This money in the game will allow the developer to review and design its role or business and create a game economy system that can be used within the game. Similar to the token economy in virtual currency, the game has game economy for game currency.

There are many ways to combine game economy and token economy, so you cannot find uniform way to combine them. Moreover, if the game economy design is left to the developer, the user cannot have their ownership of the item that purchased using the real money, in addition of the gold obtained by the user efforts.

Since we can design the sectoral economic system like game economy, we already have a cash-back system that compensates for real purchases such as gift vouchers, card points, etc., at points corresponding to cash. **We wanted to design a token economy that could be applied not only to games but also to these various fields.** Among them, games have a faster economic system than any other field in the cycle.

Therefore, before applying a similar token economy, it is considered to be the most suitable field to be able to do.

In order to apply the token economy to various fields beyond games, it is necessary to use a monetary unit with low volatility, but most of the tokens listed on the current cryptocurrency exchanges are too volatile to be suitable for our token economy. If the volatility of the tokens is too great, even if the token economy design and reward system for the game is appropriately well-designed, user participation may not be active. Therefore, a solution for this should be presented.

3 Technical Solution Offered by Orichalcos

3.1 Orichalcos Blockchain Platform

Orichalcos is a private blockchain platform that can be used in game and beyond. Compensation and history storing and trading in the games mentioned below can be applied to various areas providing points and incentives as well as games.

Recognizing the user's right on asset distribution and in-game history, Orichalcos rewards with the currency called ORIC Stone which circulates within the platform in exchange for the effort and time of the users spent on the creation of new game data. This kind of reward for gameplay induces the game to be enjoyed deeply enough and stimulates participation in new games.

The ecosystem of Orichalcos platform starts with ORIC Stone which is supplied through platform, will contributes to the game vitalization by consumed in item trading and various in-game contents. In addition, in the external exchange it can be made to an ORIC Token which is cryptocurrency. Game data will be archived and given to each user, which enables to preserve their game history and serve as a bridge between past and present.

For example, users can receive ORIC Stone in exchange for sharing their own game data to developers. And it will be utilized by developers to in advertising and operating strategies to provide more precise game services and Orichalcos also provides target marketing tools and user analysis console. In our ecosystem based on game data, the user’s history will be created from the game provided by the developer. That history will be processed into game bigdata on the private blockchain network and provided to the developer again. In this process, the value of the game experience is transformed into ORIC Stone and as a result, it creates circulation structure within the platform ecosystem. The Orichalcos ecosystem becomes bigger with the reliability of game data as the number of users in the platform increase. It will lead to more active circulation of ORIC Stone, which will contribute to the value of ORIC Token.

Thus, by combining game software with blockchain technology, Orichalcos want to build a circulative structure that allows users, developers, and platforms progress mutually.

In view of technical aspect, Orichalcos utilizes a permissioned private blockchain technology. In order to develop platform a public blockchain Hyperledger was chosen as starter. In addition, we will introduce a hierarchical consensus algorithm that combines PoET with Raft consensus algorithm to develop permission-less public blockchain in future.

For the Dual Token and blockchain system, ORIC Token and ORIC Stone, after issuing Ethereum ORIC Token will be pegged to Hyperledger Sawtooth blockchain will be used as a starter. The modified and pegged Hyperledger Sawtooth blockchain will issue ORIC Stone. We will use Oracle to supply data to the private network to take advantage of centralized external data. After separating user data from Distributed Ledger Layer in order to operate network efficiently, user data will be stored in distributed shared storage like IPFS (Inter-Planetary File System) or Storj.

In order to maintain low volatility against external fiat currency, we will operate ACB (Algorithmic Central Bank) for ORIC Stone within the platform. Therefore, after the ORIC Token Generation Event is finished to maintain the Token value in the private blockchain, the remaining tokens will be kept in the Central Treasury. That is, the token economy is designed so that the value of the token increases as the platform value grows.

The entire system will be configured as a cloud system, and approval for blockchain transactions will be made in permissioned nodes distributed worldwide. In order to develop into separate public blockchain in the future, incentives for participating nodes should be designed and reflected.

3.2 Permissioned Hierarchical Consortium Consensus Algorithm

On the blockchain system, a large number of nodes are connected to a P2P network to process a user's transaction, which can be regarded as a distributed ledger system. In a block-chain system, it is the consensus algorithm that makes it possible for all nodes to have processing records for the same transaction (Gramoli, 2017).

The consensus algorithm of the Bitcoins to which the first blockchain technique was applied was a proof-of-work method and selecting the longest chain. The Bitcoin algorithm is limited to 7 TPS at its original limit, and there is a problem that much energy is wasted due to the proof-of-work.

As mentioned above, the blockchain system that emerges after Bitcoin tends to introduce a modified consensus algorithm that alleviates performance problems and energy problems to fit the system. In the case of Ethereum, we introduced a consensus algorithm that sees the chain with the largest number of subtrees, rather than the longest chain, as the main chain.

The blockchain system is divided into permission-less type and permissioned type blockchain according to the participation restriction. Proof-of-work is indispensable in unlicensed block chains and performance and energy consumption problem. In order to overcome these problems, algorithms such as PoS (Proof-of-Stake) and PoET (Proof-of-Elapsed Time) have been developed (Lim, et al., 2018).

Consensus algorithm is a fundamental problem in fault-tolerant distributed systems. Consensus involves multiple servers agreeing on values. Once they reach a decision on a value, that decision is final. Typical consensus algorithms make progress when any majority of their servers is available; for example, a cluster of 5 servers can continue to operate even if 2 servers fail. If more servers fail, they stop making progress (but will never return an incorrect result) (Raft, 2018).

In the permissioned blockchain platform, we can believe all the participants and we can delegate the decision on a value. That is, it is possible to prescribe nodes qualified to create a block, to construct a committee composed of the nodes, and to

use a method of generating and propagating one block through agreement among committee members

If you think of the blockchain system as the storage management of the copy of the distributed ledger, you can say that it has characteristics similar to the traditional state machine replication system. The replica of SMR can divide the abnormal situation into two broad categories, one is the fail-stop and the other is the Byzantine Fault. The representative consensus algorithm assuming fail-stop is Paxos and Raft, and the representative consensus algorithm that masquerades as a Byzantine fault including malicious behavior of replica is pBFT (practical Byzantine Fault Tolerant) (Castro & Liskov, 1999).

Raft is a consensus algorithm that is designed to be easy to understand. It's equivalent to Paxos in fault-tolerance and performance. The difference is that it's decomposed into relatively independent subproblems, and it cleanly addresses all major pieces needed for practical systems (Ongaro & Ousterhout, 2014).

The Proof of Elapsed Time (PoET) Consensus method offers a solution to the Byzantine Generals Problem that utilizes a “trusted execution environment” to improve on the energy efficiency of present solutions such as Proof-of-Work (Han, 2017). The initial reference implementation of PoET released to Hyperledger was written for an abstract TEE to keep it flexible to any TEE implementation (Intel, 2014).

At a high-level, PoET stochastically elects individual peers to execute requests at a given target rate. Individual peers sample an exponentially distributed random variable and wait for an amount of time dictated by the sample. The peer with the smallest sample wins the election. Cheating is prevented through the use of a trusted execution environment, identity verification and blacklisting based on asymmetric key cryptography, and an additional set of election policies.

For the purpose of achieving distributed consensus efficiently, a good lottery function has several characteristics:

- Fairness: The function should distribute leader election across the broadest possible population of participants.
- Investment: The cost of controlling the leader election process should be proportional to the value gained from it.
- Verification: It should be relatively simple for all participants to verify that the leader was legitimately selected.

PoET is designed to achieve these goals using new secure CPU instructions which are becoming widely available in consumer and enterprise processors. PoET uses these features to ensure the safety and randomness of the leader election process without requiring the costly investment of power and specialized hardware inherent in most “proof” algorithms (Hyperledger, 2018).

Hyperledger includes an implementation which simulates the secure instructions. This should make it easier for the community to work with the software but also forgoes Byzantine fault tolerance (Intel, 2014).

PoET essentially works as follows:

1. Every validator requests a wait time from an enclave (a trusted function).
2. The validator with the shortest wait time for a particular transaction block is elected the leader.

3. One function, such as “CreateTimer”, creates a timer for a transaction block that is guaranteed to have been created by the enclave.
4. Another function, such as “CheckTimer”, verifies that the timer was created by the enclave. If the timer has expired, this function creates an attestation that can be used to verify that validator did wait the allotted time before claiming the leadership role.

The PoET leader election algorithm meets the criteria for a good lottery algorithm. It randomly distributes leadership election across the entire population of validators with distribution that is similar to what is provided by other lottery algorithms. The probability of election is proportional to the resources contributed. An attestation of execution provides information for verifying that the certificate was created within the enclave and that the validator waited the allotted time. It is suitable to implement a blockchain system that is fast and stable in games and can track accurately the movement of assets (Zhang, et al., 2017).

PoET does not have any problems at all. That is, an absolutely large number of malicious participants' nodes can still cause Byzantine problems (Chen, et al., 2017), and only systems with Intel's SGX hardware can participate (Bano, et al., 2017). As a solution to the first problem, we will use a **hierarchical consensus algorithm and integrate it with the Raft algorithm** and will study the solution for the second problem deeply.

3.3 Virtual Machine and Distributed Ledger Layer

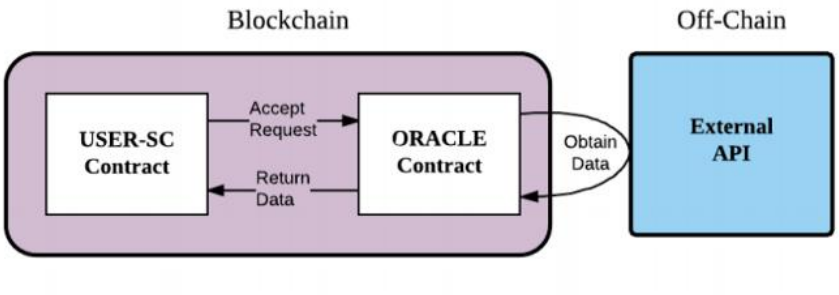
By using Hyperledger, EVM can be used without any additional development, so many existing Smart Contracts, Oracles, etc. can be utilized.

Implementing a blockchain of the entire platform of a system in which a large amount of data, such as games, is to be stored requires too much development effort. In particular, the main data of the game is stored in the central DB. In this case, the processing speed of the existing DBMS is much faster than the blockchain of the current distributed database type. User data or game history data that need to be stored is preferably stored in a separate data storage space without being stored on the block. Therefore, a block for storing user data is created, and the data area of block stores a pointer for indicating the location of database, thereby reducing the block transfer time and speeding up the transaction processing. SWAMP, IPFS or Stoj can be used with suitable smart contract or oracles. However, the speed and efficiency of the DB must be checked before implementation. Sometimes centralized DB will be faster and more efficient. Anyway, we will separate block into transaction and data area. These two split blocks will be stored in Distributed Ledger Layer. When transaction occurs, only the transaction block will be transmitted and used for transaction approval.

3.4 Oracle as Development Interface

As previously mentioned, Oracle is simply a “smart contract” that is able to interact with the outside world, in the world of Ethereum that is known as off-chain. Some people argue that Oracles aren’t exactly a real smart contract. However, smart contracts, by their nature, are able to run algorithmic calculations and store and retrieve data (Weldon, 2016).

For example, you're writing a smart contract that needs to retrieve weather data, however your contract can't make arbitrary network requests on-chain. You need something that trustable and is able to listen and respond to specific events on the blockchain. Because every node runs every calculation, it's not practical to make arbitrary network requests from an Ethereum contract. Oracles fill this void by watching the blockchain for events and responding to them by publishing the results of a query back to the contract. In this way, contracts can interact with the off-chain world (ChainLink, 2017) (Tan, 2017) (Oraclize, 2016). For more on Oracles, check out Oraclize, a FinTech company providing a 'reliable connection' between distributed apps (Oraclize, 2015).



Source: ChainLink Whitepaper — https://link.smartcontract.com/whitepaper

The game data and the block chain data are used separately, and when necessary, the data is transferred to the inside of the blockchain through Oracle to be stored or transmitted. Oracle on data migration will support commonly used languages and data formats such as JavaScript, python, Go, Node.js, and JSON.

3.5 Token Design: Token, Stone and Algorithm Central Bank

Earlier this year, a small startup company called Intangible Labs, Inc. announced their ICO white papers and raised more than 100M USD. Those who sold the Basis Token believed that the price volatility of cryptocurrencies is one of their biggest barriers to widespread adoption. Unlike the currencies using today, most cryptocurrencies do not have a mechanism to keep purchasing power stable. This means that sporadic swings in demand can cause huge changes in price (Al-Naji, et al., 2018).

We also believe that the Stone used on the platform needs to maintain stable prices in order for our platform to be widely and quickly utilized by users. An ORIC Token can be exchanged for another coin or currency in an external exchange. The Token is exchanged with the Stone on the Orichalcos platform and can be used in various ways. Stone can provide the user with various forms such as user level up, event, purchase of paid item, and item enhancement.

Hence, Stone, which is operated as a blockchain, must be stable price with respect to fiat currencies or other indices which indicate the currency price. Central banks apply monetary policy to mitigate currency volatility. The exchange from Stone to Token is performed by the Algorithmic Central Bank (ACB), which is a sort of smart contract. As with foreign exchange transactions, Algorithmic Central Bank will deduct certain fees.

The article of Myles (Snider, 2018) will be a good summary of the various aspects of the stable coin. In short, there are three types of stable coins. First type of stable coin is collateral-backed IOU like Tether, TrueUSD, Arccy, Stably. Second type is collateral-backed on-chain like BitShares, Maker, Sweetbridge, Havven, Augmint. Last type is seigniorage shares like Basis, Fragments, Carbon, Kowala. The most well-known stable coin is Tether, USDT. The Tether is not needed ACB. Tether just keep USD in bank account for escrow in accordance with Tether issuing. As in this case, stable coin need not be implemented with ACB together. However, it is necessary to minimize human intervention on coin price, and it is necessary to give transparency to pricing through automated processing by smart contract.

The simplest way to implement ACB and stable coin can be started from Quantitative Theory of Money (QTM). This basic principle is from Irving Fisher and Milton Friedman. QTM states that the price level of goods and services in an economy are directly related to the supply of money in that economy. When money is in abundant supply, the price rises (inflation), and when money is in limited supply, price deflates (Manning, 2018). Similar stable coin concept proposed by Ethereum founder Vitalik Buterin is Schelling Point (Buterin, 2014). **By adopting this concept in Orichalcos platform the algorithmic central bank can change the multiplier between ORIC Stone and Token so that the value of each Stone is fixed in unit of fiat currency.**

The remaining ORIC Tokens after the TGE are kept in the Orichalcos Central Treasury (OCT) for safekeep by the smart contract of ACB. If a user in the platform wishes to exchange Stone into Tokens, the ACB will take the Tokens corresponding to Stone out of OCT and pay the user. A developer or service provider who wants to provide Stone to the platform user can purchase a Token from the ACB and convert it to the Stone. The developer or service provider may process the Stone in a suitable form and provide it to the user.

3.6 Visual Wallet for Digital Asset Ownership and Trade

Orichalcos Visual Wallet (OVW) app is a software used to securely store, send and receive cryptocurrencies through the management of private and public cryptographic keys. It provides an interface to track balances of cryptocurrency holdings and other automated functions such as the fees per transaction, etc. It is a mobile or online based application. This makes it readily available and easily accessible with or without location-dependence and presents a convenient way to use cryptocurrencies daily.

As a cryptocurrency wallet, it can store the ORIC Token, Stone and ERC20 Token. It can be used for cryptocurrency remittance. ORIC Stone wallets will be activated by Orichalcos Network after the MVP release.

Some important features of the OVW are as follows.

- Key recovery

In the event that a user loses his smartphone or had his phone broken, OVW app has the capability to recover the private key of user's cryptocurrency wallet. What the user needs to do is to sign in to his account to recover his private key. The recovered information is zero-knowledge encrypted with a user's password and PIN, and then

stored securely on the Orichalcos Platform. A user's private key can also be recovered from the 12 mnemonic words generated upon creation of the private key.

- Mnemonic word sequence

The incorporation of the HD feature in OVW app enables the encoding of a private key into mnemonic word sequence (also referred to as a 'seed'). Mnemonic is a collection of multiple words that represent the private key in human-friendly format. These two innovations in OVW work together to make it possible to easily backup the entire wallet, simply by remembering a single paraphrase and migrating the wallet file to another provider or phone.

- Screen capture prevention

This is to protect the data of OVW. This will prevent malicious user in other applications. It is a function to prevent possibility of data leakage or personal information infringement due to copying and pasting function.

- Zero knowledge algorithm & protocol

The Zero Knowledge algorithm and protocols in the OVW app ensures that every information shared in the wallet is encrypted before it is sent to the server or shared, and the key to the encryption is also never revealed to the service provider. The zero-knowledge algorithm and protocol ensure that no key, password, files, or any other sensitive materials ever leave the system unencrypted or in reversible format.

- Item Inventory

ORIC Stone or Token will be able to bundle in-game items by developers. In this case, the ORIC Token or Stone will be implemented so that it can be viewed as an item itself rather than just a hash value.

- Social Activity i.e. voting for games and comments

Recommendations for games, game knowledge and experiences can be sold. It will be implemented for social conversations, comments to enhance social features.

- Exchange and Remittance Service

Items can be exchanged and traded. A cryptocurrency exchange and auction will be implemented. Remittance services for cryptocurrency will also be possible.

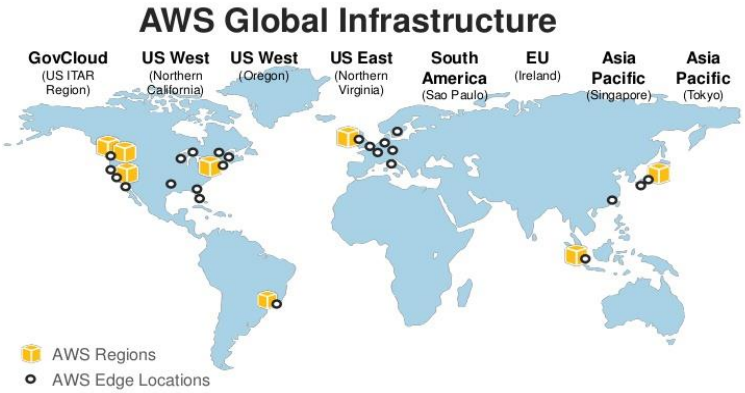
In addition to these features, we will include instant messenger features. The OVW will be upgraded to include various functions as well as storing cryptocurrency.

3.7 Cloud Infrastructure for Orichalcos Platform

The Orichalcos platform will work in a private blockchain. The Orichalcos platform's authentication server, consensus node and DLT layer must be directly built and operated until it is run as a public blockchain.

Google, Amazon and Microsoft's cloud infrastructure will be leveraged to make management easier. The platform is operated by IDC of each company built around the world. The nodes for operation will be distributed according to the structure of the worldwide Internet network such as Korea, Hong Kong, Singapore, Japan, Amsterdam, Mumbai, New York, SF and so on. Likewise, the DLT will be deployed according to the location of the Cloud server.

The operating system to be used for building each node is Linux, and each functional image will be created, deployed and updated.



MS Azure Infrastructure

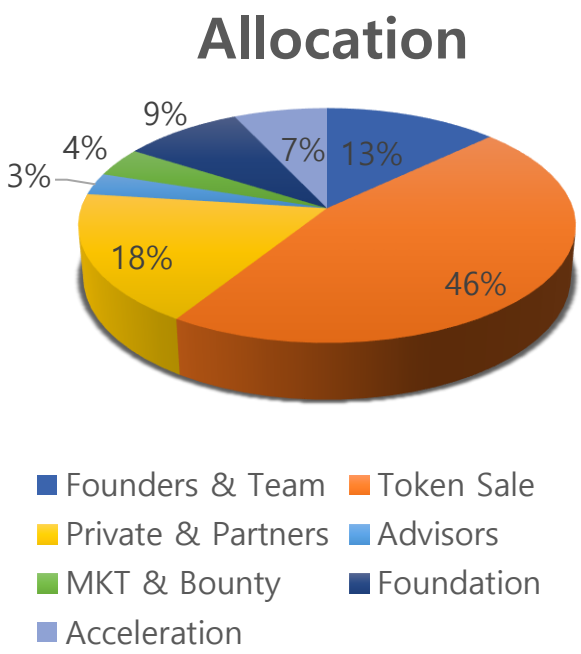
4 Token Distributions

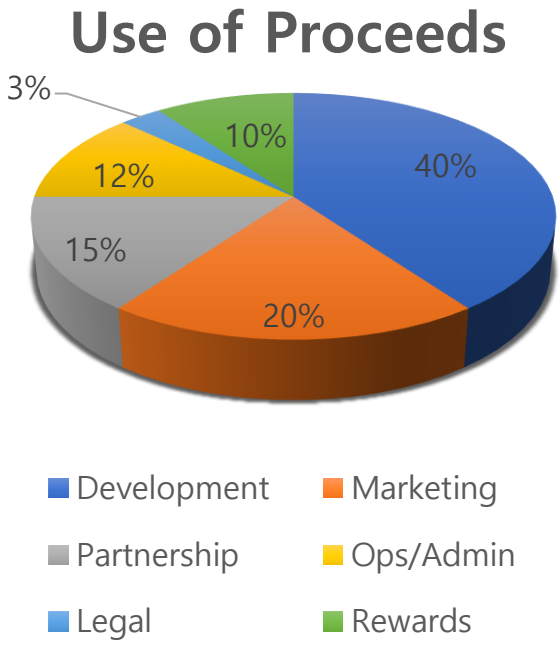
The Orichalcos Platform will be 40M USD fundraising through ICO(Initial Coin Offering). One ORIC token is selling at a price of US$0.12. A total of one billion tokens are issued, and Soft-Cap is 5M USD. Sold tokens are non-refundable and do not return coins even if they do not exceed the hard-cap.

The expected revenue from the tokens sold by Orichalcos should be determined by the individual's own judgment and responsibility, and we will not explain or affirm the dividend or profit of the token. The remaining tokens after distribution will not be incinerated but as mentioned before they will be stored in Central Treasury by smart contract.

Procured token distribution costs will be used for development, marketing, cooperation with developers and public relations companies, system operation and management, and legal review.

Partnership will be provided to developers who supply games to the Orichalcos platform and to partners who can have a direct influence on platform utilization, such as development tools or promotions. The operating and management part are the fund for the operation of the Orichalcos platform and it will be used for developers to develop technologies such as platforms, coin systems, and development tools. It will also be used for the development of in-house produced games to provide examples to external developers.





5 Executives, member and Advisors

Sungho Kim, Ph. D. (Founder and CEO)

He was the director of supercomputer development in KISTI, a government funded National institute. Former CEO of KESPER Inc., CTO of ZION Linux System CTO, VP of Crowngames and Innogrid Inc. He holds over 20 years of experience in HPC and Supercomputing, Cloud Computing, BigData, AI, Linux, decryption systems, software development and has accomplished many governments issued national projects. He also has hardware development experiences from semiconductor design, mobile devices, industrial computer (SBC) and high-performance storage systems for supercomputers. Recently, during his time as VP for a gaming company he has obtained experience in the designing of game economy, marketing and ads, as well as the monetization for social casino games.

Hyun Chul Ryu (Director of Creativeness, CPD and Co-Founder)

Hyun Chul is a game planning expert who has over 15 years' experience as a PD. A veteran in the Korean game industry, he has lead teams in small and larger companies such as Lizard Interactive, NC Soft, Smile Gate and WeMade. In his first company, LIzard Interactive, he has seen 70 times return in revenue growth while using an innovative F2P business model that was ahead of its time and is now widely adapted.
Since then, Hyun Chul has continuously been successful with his pay-per-using model through in-game content tuning for Cronos and Cross Fire among other titles. In addition to development and planning, he is a game company director with a strong passion for casual and mobile games, with a keen eye for scouting indie developers with potential.

Jae Hoon Kim (V.P. of Strategy, CSO and Co-Founder)

Former CEO of GFew Interface Inc, a web agency. Former Senior Director of strategic business department at Hancom Inc.(PLC.). Former COO of entertainment and technology company Prime Entertainment Inc.(PLC.) CEO of SNS based digital content creating & distribution service platform company Crepot Inc. As an entrepreneur and CEO with over 20 years under his belt, he holds a wide breadth experience through multiple positions (planning, development, marketing, strategy, invest and incubating, M&A and so on.) in the IT industry. He has been involved in various Windows application software businesses including Hangul, the biggest representative word processing program in Korea and office application programs. He Has been continuously challenging and experimenting Platform for Fair Profit Distribution in the Role of Market Participants with internet service for last years and is focusing on an ecosystem design that can be improved by blockchain technology.

Kweonsik Seo – Attorney at Law, Partner at DRAJU International Law Group LLC

He studied at SNU Department of Foreign Studies and holds an MA in Finance at Macquarie University, Sydney, Australia. Corporate general advisory expert for M&A and restructuring. He has been involved in the sale and acquisition of various companies including Daewoo E & C and LS through Samsung Electronics Legal & Finance team. He has experience advising many companies on derivatives trading.

Ok-Hyun Choi, Ph.D. (Advisor)

As a research committee member of the Public Procurement Service, after conducting the web service project of the national procurement system, he developed and operated an institutional management information system at the Korea Labor Welfare Corporation. He has been deeply involved in the block chain and new financial services by working at the Fintech Support Center under the Financial Supervisory Service. Currently work as PMO (Project Management Officer) of the financial system that is being implemented at the post office financial development office.

B.D. Kim, Ph.D. (Director of Research Computing at University of Virginia School of Medicine)

He worked at the National Center for Supercomputing Applications (NCSA) and the Texas Advanced Computing Center (TACC), director of Scientific Computing at Harvard University, and associate director at Harvard Medical School Research Computing Center.

Soon jung Kwon, Ph.D (Professor of Multimedia at Sogang University)

He has been working as a professor of multimedia degree at Sogang University Lifelong Education Center after lecturing at Sangmyung University and Dongguk University. Working on Digital storytelling, and game software development.

Il suk Won, Ph.D (Professor of Gaming degree at Hoseo University)

He is a professor at Hoseo University in Seoul. He is engaged in various activities such as game design, UX, and design.

Sang Hwa Lee (Professor, Dept Chair of VR Content Design, Induk University)

He majored in Industrial Design and Interaction Design at KAIST and worked as a design practitioner in Saehan Information System. Since 2004, he has been a professor at Digital Industrial Design Department of Induk University. He has been engaged in various product design and UI / UX projects. In 2018, he created and chair of VR Contents Design Department for the first time in Korea. At the same time, he is the head of the VR Convergence Center of the Specialization Projects Center and is committed to developing VR content for games and education.

TEAM MEMBERS

- Kyung Hwan Kim: (Creative Planning)
- Minjun Steve Park: (Global Marketing/Service Manager)
- Kwang Sook Yoo (Global Marketing/Ads Manager)
- Dug-Jin Jung: (Game Operation and Management)
- Kevin Pompilio (Global Business Management)
- Seung Kwan Song(Art Leader)

6 Partner Companies

SovereignWallet Network (http://sovereignwallet.network/)
Edenchain (https://edenchain.io/)
Tory Games (https://www.torygames.com/)
HNC Games (http://www.pagebrick.com/hncgames/hncgames/)
Crown Games (https://www.facebook.com/SloticaCasinoSlots/)
Patentpia (https://www.patentpia.com/kr/search/keyword)
Taketrips (https://www.taketrips.com/main)
Lawdata (http://lawdata.co.kr/)

7 Roadmap

References

1. Ahn, J., 2018. *Edenchain: The Programmable Economy Platform.* s.l., Edenchain Partners Inc. .
2. Al-Naji, N., 2018. *Medium.* [Online] Available at: https://medium.com/basis-blog/introducing-basis-a-stable-cryptocurrency-with-an-algorithmic-central-bank-7a795393a525
3. Al-Naji, N., Diao, L. & Chen, J., 2018. *BASIS.* [Online] Available at: https://www.basis.io/
4. IBM, 2018. *Blockchain for supply chain.* [Online] Available at: https://www.ibm.com/blockchain/industries/supply-chain
5. Aspnes, J., Jackson, C. & Krishnamurthy, A., 2005. Exposing computationally-challenged Byzantine impostors.. *Technical report.*
6. Bano, S. 외., 2017. *SoK: Consensus in the Age of Blockchain.*, ArXiv.
7. Bonneau, J. et al., 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE Symposium on Security and Privacy,* May.
8. Buterin, V., 2013. Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform.
9. Buterin, V., 2014. *Ethereum.* [Online] Available at: https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/
10. Buterin, V., 2014. *Ethereum Blog.* [Online] Available at: https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/
11. Castro, M. & Liskov, B., 1999. *Practical Byzantine Fault Tolerance,* New Orleans: Proc. 3rd Symp. on OSDI.
12. ChainLink, 2017. *ChainLink.* [Online] Available at: https://chain.link/
13. Chaum, D., 1982. Blind signatures for untraceable payments. *CRYPTO.*
14. Chen, L. 외., 2017. *On Security Analysis of Proof-of-Elapsed-Time(PoET).*, Spinger Link.
15. Dai, W., 1998. *b-money,* s.l.: s.n.
16. David, C., A., F. & M., N., 1990. Untraceable electronic cash. *CRYPTO.*
17. Dwork, C. & Naor, M., 1992. Pricing via processing or combatting junk mail. *CRYPTO.*
18. Ephraim, F., 2018. A Framework for Blockchain-Based Applications. *ArXiv,* 2 Mar.
19. Garay, J. A., Kiayias, A. & Leonardos, N., 2017. *The Bitcoin Backbone Protocol: Analysis and Applications.* , Proc. Eurocrypt 2015.
20. Gartner, 2015. *Gartner.* [Online] Available at: https://www.gartner.com/newsroom/id/3146018.
21. Goldschlag, D. M. & Stubblebine, S. G., 1998. Publicly Verifiable Lotteries: Applications of Delaying Functions.. *Financial Cryptography.*
22. Gramoli, V., 2017. *From Blockchain Consensus Back to Byzantine Consensus,* Elsevier.
23. Han, D., 2017. *Intel SGX and its Network Applications,* Security@KAIST.
24. Hegadekatti, K. & G., Y. S., 2017. *The programmable Economy: Envisaging an Entire Planned Economic System as a Single Computer through Blockchain Networks,* MPRA.

25. Hyperledger, 2018. *Hyperledger Sawtooth.* [Online]
Available at: https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html
26. Intel, 2014. *Intel.* [Online]
Available at: https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf
27. Intel, 2014. *Intel Sawtooth Lake.* [Online]
Available at: https://intelledger.github.io/
28. Jason, C., 2017. [Online]
Available at: https://www.forbes.com/sites/delltechnologies/2017/06/27/how-blockchain-could-revolutionize-the-internet-of-things/#225505276eab
29. joce00, 2018. *STEEMIT.* [Online]
Available at: https://steemit.com/kr/@joceo00/token-economy
30. Lim, J., Yoo, H., Kwak, J. & Kim, S., 2018. *Blockchain and Consensus Algorithm.* Taejeon, ETRI.
31. Manning, M., 2018. *TGDaily.* [Online]
Available at: https://www.tgdaily.com/technology/can-the-usdx-protocol-replace-central-banks-with-an-algorithm
32. Marco, . I. & Karim, L. R., 2017. The Truth About Blockchain. *Harvard Business Review.*
33. mechuriya, 2018. *STEEMIT.* [Online]
Available at: https://steemit.com/kr/@mechuriya/declaration-of-token-economy
34. Morabito, V., 2017. *Business Innovation Through Blockchain.* s.l.:Spinger.
35. Moreno, P. d. l. C., 2017. *Medium.* [Online]
Available at: https://blog.icofunding.com/tokens-and-tokenomics-the-magic-of-icos-a7a886ca323c
[Accessed 2018].
36. Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Oct.
37. Okamoto, T. & Ohta, K., 1992. Universal electronic cash. *CRYPTO.*
38. Ongaro, D. & Ousterhout, J., 2014. *In Search of an Understandable Consensus Algorithm.* s.l., Stanford University.
39. Oraclize, 2015. *Oraclize.* [Online] Available at: http://docs.oraclize.it/#home
40. Oraclize, 2016. *Medium.* [Online]
Available at: https://blog.oraclize.it/understanding-oracles-99055c9c9f7b
41. Raft, 2018. [Online]
Available at: https://raft.github.io/
42. Ralph, M. C., 1980. Protocols for Public Key Cryptosystems. *IEEE Symp. on Security and Privacy,* 4.
43. Rouse, M., 2018. *Techtarget.com.* [Online]
Available at: https://searchcio.techtarget.com/definition/programmable-economy
44. Sander, T., Ta-Shma, A. & Yung, M., 2001. Blind, auditable membership proofs.. *Financial Cryptography.*
45. Seyoung, H., Sangrae, C. & Soohyeong, K., 2017.비트코인 후 블록체인. *초연결 지능 인프라 특집*, 2.
46. Snider, M., 2018. *Multicoin.capital: An Overview of StableCoins.* [Online]
Available at: https://multicoin.capital/2018/01/17/an-overview-of-stablecoins/

47. Steve, M., 2017. [Online]
Available at: https://www.fastcompany.com/40449268/will-blockchain-revolutionize-global-real-estate-next
48. Szabo, N., 1997. Formalizing and securing relationships on public networks.. *First Monday,* 2(9).
49. Tan, K., 2017. *Kendrick Tan.* [Online]
Available at: https://kndrck.co/posts/ethereum_oracles_a_simple_guide/
50. Weldon, J., 2016. *Medium.* [Online]
Available at: https://medium.com/@mustwin/building-an-oracle-for-an-ethereum-contract-6096d3e39551
51. Wikipedia, 2018. *Wikipedia.* [Online]
Available at: https://en.wikipedia.org/wiki/Tokenization_(data_security)
52. Wikipeida, 2018. *Wikipedia.* [Online]
Available at: https://en.wikipedia.org/wiki/Money
53. Zhang, F. et al., 2017. *REM: Resource-Efficient Mining for Blockchain.*, Cornell University.

Disclaimer

This document is a technical whitepaper (the “Whitepaper” or “Paper”) setting out and illustrating the current and future projects (the “Project”) of Orichalcos Foundation (“Orichalcos” or the “Foundation”) and in connection with the development of its platform (the “Platform”) to potential token holders in connection with the proposed ORIC token (the “ORIC Token” or “Token”) launch (the “Token Generation Event”).

.**.

Nothing in this Whitepaper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction. This document is not composed in accordance with, and is not subject to, Laws or regulations of any jurisdiction which are designed to protect investors.
This Paper is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any State, Country or other jurisdiction where such distribution, publication, availability or use would be contrary to Law or regulation.
The manner of distributing this Paper may be restricted by Law or regulation in certain Countries. Persons into whose possession this Paper may come are required to inform themselves about and to observe such restrictions. By accessing this Paper, a recipient hereof agrees to be bound by the limitations provided by this Paper.
The information set forth in this Paper may not be exhaustive and does not imply any elements of a contractual relationship. The sole purpose of this Paper is to provide relevant and reasonable information to potential Token holders in order for them to determine whether to undertake a thorough analysis of the Foundation, the Project and the Platform with the intent of acquiring ORIC Tokens. This Paper is for information purposes only and is not a statement of future intent.
This Paper is only available on www.orichalcos.io and may not be redistributed, reproduced or passed on to any other person or published, in part or in whole, for any purpose, without the prior, written consent of Orichalcos.

.**.

Unless expressly specified otherwise, the Foundation, the Project and the Platform set out in this Paper are currently under development and are not currently in deployment. No warranties or representations are made as to the successful development or implementation of the Foundation, the Project and the Platform and of the subjacent technologies and innovations, or achievement of any other activities described in the Paper, and any warranties implied by Law or otherwise, are disclaimed and waived to the extent permitted by Law. No person is entitled to rely on the contents of this Paper or any inferences drawn from it, including in relation to any interactions with Orichalcos or the technologies mentioned in this Paper.
All liabilities for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions relating to Orichalcos, the Platform or the Project contained in this Paper or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care, are disclaimed and waived.
Certain statements, estimates, information and opinion contained in this Whitepaper constitute forward-looking
statements or information. Such forward-looking statements or information involve known and unknown risks and uncertainties which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements.
The information contained in this Paper derived from data obtained from sources believed to be reliable is given in good faith, but no warranties, guarantees, or representations are made with regard to the accuracy, completeness or suitability of the information presented. It should not be relied upon, and shall not confer rights or remedies upon, you or any of your employees, creditors, or any other

person.
Any opinions expressed in this Paper reflect the current judgment of its authors and do not necessarily represent the opinion of Orichalcos and may change without notice. There is no obligation whatsoever to amend, modify or update this Paper or to otherwise notify a reader or recipient thereof in the event that any matter stated herein, or any opinion, projection, forecast or estimate set forth herein, changes or subsequently becomes inaccurate.
Orichalcos, its directors, employees, contractors and representatives do not have any responsibility or liability to any person or recipient (whether by reason of negligence, negligent misstatement or otherwise) arising from any statement, estimates, opinion or information, expressed or implied, arising out of, contained in or derived from or omission from this Paper. Neither Orichalcos nor its advisors have independently verified any of the information, including the expectations and projections contained in this Paper.
Each recipient has to rely solely on its own knowledge, investigation, judgment and assessment of the matters which are the subject of this Paper and any information which is made available in connection with any further enquiries and to satisfy itself as to the accuracy and completeness of such matters. It is recommended to obtain advice from experts such as legal or tax advisors.
Whilst every effort is made to ensure that statements of facts made in this Paper are accurate, all estimates, projections, forecasts, prospects, expressions of opinion and other subjective judgments contained in this Paper are based on assumptions considered to be reasonable as of the date of the document in which they are contained and must not be construed as a representation that the matters referred to therein will occur. Any plans, projections or forecasts mentioned in this Whitepaper may not be achieved due to multiple risk factors including, without limitation, defects in technology developments, legal or regulatory exposure, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information.
Orichalcos may provide hyperlinks to websites of entities mentioned in this Paper, however the inclusion of a link does not imply that Orichalcos endorses, recommends or approves any material on the linked page or accessible from it. Such linked websites are accessed entirely at recipient's own risk. Orichalcos does not accept responsibility whatsoever for any such material, nor for consequences of its use.
The Whitepaper, written in English language, is the primary official source of information about the ORIC Token launch. The information contained herein may be translated into other languages or used in the course of written or verbal communications with existing and prospective customers, partners, etc. In the course of such translation or communication some of the information contained herein may be lost, corrupted, or misrepresented and, in any case, the accuracy of such alternative communications cannot be guaranteed. In the event of any conflicts or inconsistencies between such translations and communications and this official English language Whitepaper, the provisions of this English language original Paper shall prevail.
Notwithstanding the above, if you are a green card holder of the United States or a United States citizen or permanent resident of the United States (tax or otherwise), or you have a primary residence or domicile in the United States (tax or otherwise), including Puerto Rico, the U.S. Virgin Islands or any other possession of the United States, or you are a citizen or permanent resident of the Republic of Singapore (tax or otherwise), or you have a primary residence or domicile in the Republic of Singapore or you are a citizen or permanent resident of Canada (tax or otherwise), or you have a primary residence or domicile in Canada, or you are a citizen or permanent resident of Hong Kong (tax or otherwise), or you have a primary residence or domicile in Hong Kong, or you are a citizen or permanent resident of People's Republic of China (tax or otherwise), or you have a primary residence or domicile in the People's Republic of China, you are not eligible to acquire ORIC Tokens in any form and/or by any means.
The same applies if you are one of the owners or beneficiaries of the company, whether or not you are authorized to act on its behalf.